

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 SUBJECT PREMISES at 13742 97th Ave. NE
 Kirkland, WA 98034

Case No. MJ20-387

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The SUBJECT PREMISES as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Title 18, U.S.C. § 2252 (a)(2)
 Title 18, U.S.C. § 2252(a)(4)(B)

Offense Description


Receipt or Distribution of Child Pornography
 Possession of Child Pornography

The application is based on these facts:

- ☒ See attached Affidavit continued on the attached sheet

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.


 Applicant's signature

Ingrid Arbuthnot-Stohl, Special Agent
 Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 06/29/2020


 Judge's signature

City and state: Seattle, Washington

Michelle L. Peterson, United States Magistrate Judge
 Printed name and title

ATTACHMENT A
(SUBJECT PREMISES)

The physical address of the SUBJECT PREMISES is 13742 97th Ave., NE, Kirkland, WA 98034, and is more fully described as a property containing a two-story, single-family home with an attached carport, yellow-orangish and blue color siding with white trim. The front door is located off of the carport with a small box to the side of the door and the numbers 13742 on a plaque above the box. The residence is at the end of a cul-de-sac.



1 The search is to include all rooms, persons, garages, vehicles, or outbuildings
2 located on the SUBJECT PREMISES, as well as any digital device(s) or other electronic
3 storage media found therein or thereon.
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT B**(PROPERTY TO BE SEIZED)**

Evidence, fruits, and instrumentalities of violations 18 U.S.C. §§ 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), as follows:

- a. Items, records, or information³ relating to visual depictions of minors engaged in sexually explicit conduct;
- b. Items, records, or information relating to the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;
- c. Items, records, or information concerning communications about the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;
- d. Items, records, or information concerning communications about the sexual abuse or exploitation of minors;
- e. Items, records, or information related to communications with or about minors;
- f. Items, records, or information concerning the identities and contact information (including mailing addresses) of any individuals involved in the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct, saved in any form;
- g. Items, records, or information concerning occupancy, residency or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence,

³ As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

1 purchase or lease agreements, diaries, statements, identification documents,
2 address books, telephone directories, and keys;

3 h. Items, records, or information concerning the ownership or use of computer
4 equipment found in the SUBJECT PREMISES, including, but not limited
5 to, sales receipts, bills for internet access, handwritten notes, and computer
6 manuals;

7 i. Any digital devices or other electronic storage media⁴ and/or their
8 components including:

9 i. any digital device or other electronic storage media capable of being
10 used to commit, further, or store evidence, fruits, or instrumentalities
11 of the offenses listed above;

12 ii. any magnetic, electronic or optical storage device capable of storing
13 data, including thumb drives, SD cards, or external hard drives;

14 iii. any physical keys, encryption devices, dongles and similar physical
15 items that are necessary to gain access to the computer equipment,
16 storage devices or data; and

17 iv. any passwords, password files, test keys, encryption codes or other
18 information necessary to access the computer equipment, storage
19 devices or data.

20 j. For any digital device or other electronic storage media whose seizure is
21 otherwise authorized by this warrant, and any digital device or other
22 electronic storage media that contains or in which is stored records or
23 information that is otherwise called for by this warrant:

24 i. evidence of who used, owned, or controlled the digital device or
25 other electronic storage media at the time the things described in this
26 warrant were created, edited, or deleted, such as logs, registry
27

28 ⁴ The term “digital devices” includes all types of electronic, magnetic, optical, electrochemical,
or other high speed data processing devices performing logical, arithmetic, or storage functions,
including desktop computers, notebook computers, mobile phones, tablets, server computers, and
network hardware. The term “electronic storage media” includes any physical object upon
which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash
memory, CD-ROMs, and other magnetic or optical media.

1 entries, configuration files, saved usernames and passwords,
2 documents, browsing history, user profiles, email, email contacts,
3 “chat,” instant messaging logs, photographs, and correspondence;

4 ii. evidence of software that would allow others to control the digital
5 device or other electronic storage media, such as viruses, Trojan
6 horses, and other forms of malicious software, as well as evidence of
7 the presence or absence of security software designed to detect
8 malicious software;

9 iii. evidence of the lack of such malicious software;

10 iv. evidence of the attachment to the digital device of other storage
11 devices or similar containers for electronic evidence;

12 v. evidence of counter-forensic programs (and associated data) that are
13 designed to eliminate data from the digital device or other electronic
14 storage media;

15 vi. evidence of the times the digital device or other electronic storage
16 media was used;

17 vii. passwords, encryption keys, and other access devices that may be
18 necessary to access the digital device or other electronic storage
19 media;

20 viii. documentation and manuals that may be necessary to access the
21 digital device or other electronic storage media or to conduct a
22 forensic examination of the digital device or other electronic storage
23 media;

24 ix. records of or information about the Internet Protocol used by the
25 digital device or other electronic storage media;

26 x. records of internet activity, including firewall logs, caches, browser
27 history and cookies, “bookmarked” or “favorite” web pages, search
28 terms that the user entered into any internet search engine, and
records of user-typed web addresses.

xi. contextual information necessary to understand the evidence
described in this attachment.

1 This warrant authorizes a review of electronic storage media and electronically
2 stored information seized or copied pursuant to this warrant in order to locate evidence,
3 fruits, and instrumentalities described in this warrant. The review of this electronic data
4 may be conducted by any government personnel assisting in the investigation, who may
5 include, in addition to law enforcement officers and agents, attorneys for the government,
6 attorney support staff, and technical experts. Pursuant to this warrant, the FBI may
7 deliver a complete copy of the seized or copied electronic data to the custody and control
8 of attorneys for the government and their support staff for their independent review.

9 THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE
10 MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS
11 SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO
12 THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC
13 STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL
14 ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE
15 CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR
16 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED
17 CRIMES.
18
19
20
21
22
23
24
25
26
27
28

INTRODUCTION AND AGENT BACKGROUND

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

PURPOSE OF AFFIDAVIT

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants for the following location and persons:

(1) The premises located at 13742 97th Ave. NE, Kirkland, WA 98034 (hereinafter the "SUBJECT PREMISES"), further described in Attachment A, which is incorporated herein by reference.

3. As set forth below, there is probable cause to believe that the SUBJECT PREMISES will contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) (hereinafter the "TARGET OFFENSES"). I seek authorization to search and seize the items specified in Attachment B, which is incorporated herein by reference.

4. The information in this affidavit is based upon the investigation I have conducted in this case, my conversations with other law enforcement officers who have engaged in various aspects of this investigation, and my review of reports written by other law enforcement officers involved in this investigation. Because this affidavit is being submitted for the limited purpose of securing search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are sufficient to establish probable cause to support the issuance of the requested warrants. When the statements of others are set forth in this affidavit, they are set forth in substance and in part.

DEFINITIONS

5. The following definitions apply to this Affidavit:

Internet Service Providers

a. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the

Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial up, broadband-based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “email address,” an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISP's servers.

Internet Protocol (IP) Addresses

b. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer connected to the Internet must be assigned an IP address so that the Internet traffic sent from, and directed to, that computer may be properly directed from its source to its destination. Most ISPs control the range of IP addresses.

PEER-TO-PEER (P2P) FILE SHARING

6. Peer to peer (P2P) file sharing is a method of communication available to internet users through the use of special software programs. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer system to another while connected to a network, usually on the internet. There are multiple types of P2P file sharing networks on the internet. To

1 connect to a particular P2P file-sharing network, a user first obtains a P2P client software
2 program for a particular P2P file sharing network, which can be downloaded from the
3 internet. A particular P2P file-sharing network may have many different P2P client
4 software programs that allow access to that particular P2P file-sharing network.
5 Additionally, a particular P2P client software program may be able to access multiple
6 P2P file sharing networks. These P2P client software share common protocols for
7 network access and file sharing. The user interface, features, and configurations may
8 vary between clients and versions of the same client.

9 7. In general, P2P client software allows the user to set up file(s) on a
10 computer to be shared on a P2P file-sharing network with other users running compatible
11 P2P client software. A user can also obtain files by opening the P2P client software on
12 the user's computer and conducting a search for files that are of interest and currently
13 being shared on a P2P file-sharing network.

14 8. Some P2P file sharing networks are designed to allow users to download
15 files and frequently provide enhanced capabilities to reward the sharing of files by
16 providing reduced wait periods, higher user ratings, or other benefits. In some instances,
17 users are not allowed download files if they are not sharing files. Typically, settings
18 within these programs control sharing thresholds.

19 9. Typically, during a default installation of a P2P client software program,
20 settings are established which configure the host computer to share files. Depending
21 upon the P2P client software used, a user may have the ability to reconfigure some of
22 those settings during installation or after the installation has been completed.

23 10. Typically, a setting establishes the location of one or more directories or
24 folders whose contents (digital files) are made available for distribution to other P2P
25 clients. In some clients, individual files can also be shared.

26 11. Typically, a setting controls whether or not files are made available for
27 distribution to other P2P clients.

1 12. Typically, a setting controls whether or not users will be able to share
2 portions of a file while they are in the process of downloading the entire file. This feature
3 increases the efficiency of the network by putting more copies of the file segments on the
4 network for distribution.

5 13. Typically, files being shared by P2P clients are processed by the client
6 software. As part of this processing, a hashed algorithm value is computed for each file
7 and/or piece of a file being shared (dependent on the P2P file sharing network), which
8 uniquely identifies it on the network. A file (or piece of a file) processed by this hash
9 algorithm operation results in the creation of an associated hash value often referred to as
10 a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent
11 that two or more files with the same hash value are identical copies of the same file
12 regardless of their file names. By using a hash algorithm to uniquely identify files on a
13 P2P network, it improves the network efficiency. Because of this, typically, users may
14 receive a selected file from numerous sources by accepting segments of the same file
15 from multiple clients and then reassembling the complete file on the local computer.
16 This is referred to as multiple source downloads. This client program succeeds in
17 reassembling the file from different sources only if all the segments came from exact
18 copies of the same file. P2P file sharing networks use hash values to ensure exact copies
19 of the same files are used during this process.

20 14. P2P file sharing networks, including the BitTorrent network, are frequently
21 used to trade digital files of child pornography. These files include both images and
22 movie files.

23 15. The BitTorrent network is a very popular and publicly available P2P
24 sharing network. Most computers that are part of this network are referred to as “peers.”
25 The terms “peers” and “clients” can be used interchangeably when referring to the
26 BitTorrent network. A peer can simultaneously provide files to some peers while
27 downloading files from other peers.

1 16. The BitTorrent network can be accessed by computers running many
2 different client programs, some of which include the BitTorrent client program, uTorrent
3 client program, and Vuze client program. These client programs are publicly available
4 and free P2P client software programs that can be downloaded from the internet. There
5 are also BitTorrent client programs that are not free. These BitTorrent client programs
6 share common protocols for network access and file sharing. The user interfaces,
7 features, and configuration may vary between clients and versions of the same client.

8 17. During the installation of typical BitTorrent network client programs,
9 various settings are established which configure the host computer to share files.
10 Depending upon the BitTorrent client used, a user may have the ability to reconfigure
11 some of those settings during installation or after installation has been completed.
12 Typically, a setting establishes the location of one or more directories of folders whose
13 contents (files) are made available to other BitTorrent network users to download.

14 18. In order to share a file or set of files on a BitTorrent network, a "Torrent"
15 file needs to be created by the user that initially wants to share the file or set of files. A
16 "Torrent" is typically a small file that describes the file(s) that are being shared, which
17 may include information on how to locate the file(s) on the BitTorrent network. A
18 typical BitTorrent client will have the ability to create a "Torrent" file. It is important to
19 note that the "Torrent" file does not contain the actual file(s) being shared, but
20 information about the file(s) described in the "Torrent," such as the name(s) of the file(s)
21 being referenced in the "Torrent" and the "info hash" of the "Torrent." The "info hash"
22 is a SHA-1 hash value of the set of data describing the file(s) referenced in the "Torrent,"
23 which include the SHA-1 hash value of each piece, the file size, and the file name(s).
24 The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent
25 network. The "Torrent" file may also contain information on how to locate file(s)
26 referenced in the "Torrent" by identifying "Trackers." "Trackers" are computers on the
27 BitTorrent network that collate information about peers/clients that have recently
28 reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only

1 a pointer to peers/clients on the network who may be sharing part, or all of the file(s)
2 referenced in the "Torrent." It is important to note that the "Trackers" do not actually
3 have the file(s) and are used to facilitate the finding of other peers/clients that have the
4 entire file(s) or at least a portion of the file(s) available for sharing. It should also be
5 noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to
6 locate peers/clients that have file(s) being shared from a particular "Torrent" file. There
7 are many publicly available servers on the Internet that provide BitTorrent tracker
8 services.

9 19. Once a "Torrent" is created, in order to share the file(s) referenced in the
10 "Torrent" file, a user typically makes the "Torrent" available for other users, such as via
11 websites on the Internet.

12 20. In order to locate "Torrent" files of interest, a typical user will use keyword
13 searches within the BitTorrent network client itself or on websites hosting "Torrents."
14 Once a "Torrent" file is located that meets the keyword search criteria, the user will
15 download the "Torrent" file to their computer. Alternatively, a user can also search for
16 and locate "magnet links," which is a link that enables the BitTorrent network client
17 program itself to download the "Torrent" to the computer. In either case, a "Torrent" file
18 is downloaded to the user's computer. The BitTorrent network client will then process
19 that "Torrent" file in order to find "Trackers" or utilize other means that will help
20 facilitate finding other peers/clients on the network that have all or part of the file(s)
21 referenced in the "Torrent" file. It is again important to note that the actual file(s)
22 referenced in the "Torrent" are actually obtained directly from other peers/clients on the
23 BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the
24 network return information about remote peers/clients that have recently reported they
25 have the same file(s) available for sharing (based on SHA-1 "info hash" value
26 comparison), or parts of the same file(s), referenced in the "Torrent," to include the
27 remote peers/clients Internet Protocol (IP) addresses.

21. For example, a person interested in obtaining child pornographic images on the BitTorrent network would open the BitTorrent client application on his/her computer and conduct a keyword search for files using a term such as “preteen sex.” (It should be noted that this search term may not have been used in this investigation.) The results of the torrent search are typically returned to the user’s computer by displaying them on the torrent hosting website. The hosting website will typically display information about the torrent, which can include the name of the torrent file, the name of the file(s) referenced in the torrent file, the file(s) size, and the “info hash” SHA-1 value of the torrent file. The user then selects a torrent of interest to download to their computer. Typically, the BitTorrent client program will then process the torrent file. The user selects from the results displayed the file(s) they want to download that were referenced in the torrent file. Utilizing trackers and other BitTorrent network protocols (such as Distributed Hash Tables, Peer Exchange, and Local Peer Discovery), peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the torrent file available for sharing. The file(s) is then downloaded directly from the computer(s) sharing the file. Typically, once the BitTorrent network client has downloaded part of the file(s), it may immediately begin sharing the file with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives “pieces” with the exact SHA-1 piece hash described in the torrent file. During the download process, a typical BitTorrent client program displays the Internet Protocol address of the peers/clients that appear to be sharing part or all of the file(s) referenced in the torrent file or other methods utilized by the BitTorrent network protocols. The downloaded file is then stored in the area previously designated by the user and/or the client program. The downloaded file(s), including the torrent file, will remain until moved or deleted.

22. Law Enforcement has created BitTorrent network client programs that obtain information from trackers about peers/clients recently reporting that they are involved in sharing digital files of known actual child pornography (based on the “info

1 hash" SHA-1 hash value), which then allows the downloading of a file from a single IP
2 address (as opposed to obtaining the file from multiple peers/clients on the network.)
3 This procedure allows for the detection and investigation of those computers involved in
4 sharing digital files of known actual child pornography on the BitTorrent network.

5 23. During the query and/or downloading process from a remote BitTorrent
6 network client, certain information may be exchanged between the investigator's client
7 and the remote client they are querying and/or downloading a file from. Such as 1) the
8 remote client's IP address; 2) a confirmation from the remote client that they have pieces
9 of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being
10 reported as shared from the remote client program; and 3) the remote client program and
11 version. This information may remain on the remote client's computer system for long
12 periods of time. The investigator has the ability to log this information. A search can
13 later be conducted on a seized computer system(s) for this information, which may
14 provide further evidence that the investigator's client communicated with the remote
15 client.

16 **PROBABLE CAUSE**

17 24. In February 2020, while acting in an undercover capacity, I used an
18 automated law enforcement version of a publicly available Internet based peer to peer
19 (P2P) file sharing program, known as BitTorrent, to identify P2P users possessing and
20 distributing child pornography image and video files. This law enforcement version of
21 BitTorrent, described below, is similar to standard BitTorrent clients but instead of
22 seeking out different computers offering files not completely downloaded or if only one
23 or a few parts of the file are downloaded from a given computer, the law enforcement
24 version of BitTorrent will make repeated attempts to contact the subject IP address and
25 download additional parts of the file. These repeated attempts can sometimes transpire
26 over a period of several days. If a suspected child pornography file is large, such as a
27 high definition video or a large image file set (image file sets are files containing
28 numerous single image files stored within one or more separate folders), the law

1 enforcement version of BitTorrent, due to system constraints, sometimes fails to
2 download the entire file but is successful in downloading a number of the designated
3 parts of the file. When this occurs with a video file, the downloaded file parts are often
4 still viewable as short video segments and it is still possible to establish that the video file
5 contains child pornography. When this occurs with large image file sets, the downloaded
6 file parts are often individually viewable images, which can be reviewed to establish that
7 the image file set contains child pornography.

8 25. Between February 6, 2020, and April 28, 2020, I used the automated law
9 enforcement version of BitTorrent to establish multiple single source connections with
10 the IP address 73.11.165.212 (the SUBJECT IP ADDRESS) and successfully download
11 multiple files. Below are examples of suspected child pornography files download from
12 the SUBJECT IP ADDRESS that I have viewed, but these reflect a small fraction of the
13 total number of files of suspected child pornography downloaded from the SUBJECT IP
14 ADDRESS during this period :

15 **File 1 (downloaded February 7, 2020):**

16 This video is approximately 4 minutes and 59 seconds long. It features a
17 pubescent female approximately 11-13 years old based upon minimal breast
18 development, minimal pubic hair, minimal hip development, overall body size and
19 facial features. The video begins with the girl fully clothed on a bed. The victim
20 performs a strip tease until she is fully undressed. The victim then lays on her
21 back and spreads her legs wide to expose her vagina then flips over to expose her
22 anus which the camera zooms in on her. The victim continues to get into various
23 positions with her legs spread, legs over her head, in a back bend, and other
24 positions, which the camera zooms in on. The video ends with the victim
25 performing a backbend where her vagina is pointed towards the camera and is the
26 focal point of the frame.

27 **File 2 (downloaded February 7, 2020):**

28 This file is an image which is part of a larger series of photos featuring the same
victim. The image features a prepubescent female approximately 9-11 years old
based upon the lack of breast development, lack of pubic hair, lack of hip
development, overall body size, and facial features. The victim is sitting on the
fulcrum of a prop seasaw that appears to part of a circus-themed background. The
victim is wearing a half top that exposes her breasts, striped knee high stockings,

1 and metallic high heels. Her legs are spread wide to expose her vaginal area,
2 which is the focal point of the image.

3 **File 3 (downloaded February 8, 2020):**

4 This file is an image of a prepubescent female approximately 9-11 years old based
5 upon the lack of pubic hair, lack of breast and hip development, overall facial
6 features and body size. The image is part of a larger series of images featuring the
7 same victim. The victim is sitting on the ground of a set that features a tropical
8 floral theme. The victim is wearing a covering that is slung crossways across her
9 torso. One breast is visible, the other is covered by the strip of fabric. The victim
is sitting her legs spread such that her vaginal area is visible and the focal point of
the picture. In the upper righthand corner is the superimposed stamp that reads
"LS Models.com/http:www.ls-models.com".

10 **File 4 (downloaded April 15, 2020):**

11 This video is approximately 59 minutes and 58 seconds long. It features a
12 prepubescent female approximately 11-12 years old, based up on the lack of pubic
13 hair, lack of breast and hip development, overall body size and facial features.
14 The video begins with the victim wearing a silk bathroom and metallic high heels.
15 She disrobes so that she is completely naked and spreads body oil all over her
16 body. Throughout the video she dances and gets in various positions. Based upon
17 intermittent flashes of light, it appears she is posing for a photo shoot. Her
18 mannerisms suggest she is receiving instruction from someone off camera who is
19 telling her how to pose. Approximately 25 minutes into the video she sits on a
20 chair, spreading her legs so that her vaginal area is exposed and the focal point of
the shot. At approximately 53 minutes in, she bends her knees and spreads her
legs to expose her vaginal area and then puts her hands on her vaginal area.
Towards the end of the video, she brings her foot up by her head to more fully
expose her vaginal area.

21 **File 5 (downloaded April 22, 2020):**

22 This video is approximately 13 minutes and 15 seconds long. It features a
23 pubescent female approximately 12-14 years old based up on the minimal breast
24 development, minimal pubic hair development, minimal hip development, overall
25 body size, and facial features. The victim begins by stripping and fondling her
26 breasts. Approximately 5 minutes into the video, the victim begins performing
27 oral sex on a board-mounted erect dildo. Approximately 8 minutes and 40
28 seconds into the video, she removes her underwear so that she is wearing only
thigh high red stockings. She spreads her legs to fully expose her vagina.
Approximately 10 minutes into the video she obtains what appears to be a black
marker pen. She bends over the camera zooms in on her exposed vagina and anus.

1 The victim inserts the marker into her anus and begins to manually rub her vaginal
2 area. The remaining moments of the video zoom in on her vagina and anus for
3 several moments. The victim then faces the camera and blows a kiss.

4 26. A query of a publicly available database revealed the SUBJECT IP
5 ADDRESS belonged to Comcast Communications.

6 27. In response to administrative summons seeking subscriber information for
7 the SUBJECT IP ADDRESS, Comcast Communications reported that on the dates the
8 above files were downloaded, the SUBJECT IP ADDRESS was assigned to Brad Ulrich
9 with a service address at the 13742 97th Ave NE, Kirkland, WA 98034, the SUBJECT
10 PREMISES.

11 28. Washington State Department of License information shows that Robert B.
12 Ulrich has a valid Washington driver license listing the SUBJECT PREMISES as his
13 address. Other law enforcement tools and open source searches indicate Robert B. Ulrich
14 regularly uses his middle name as his first name, so that his name appears as Brad Ulrich.
15 Brad Ulrich appears to be the only adult resident of the SUBJECT PREMISES. From my
16 investigation, it appears Ulrich has two minor children who may reside at the SUBJECT
17 PREMISES on a part-time basis.

18 29. Open source property records show the residence at 13742 97th Ave NE,
19 Kirkland, WA 98034 is currently owned by Robert Bradley Ulrich.

20 30. While conducting surveillance at the SUBJECT PREMISES on May 28,
21 2020, agents saw a white Acura SUV bearing the plate BEE5974 parked under the
22 carport of the SUBJECT PREMISES. Washington State Department of License
23 information indicated that vehicle is currently owned by Pinnacle Health PS and
24 registered to the SUBJECT PREMISES. From my investigation, I have learned that
25 Pinnacle Health PS is a chiropractic business located in Bellevue, Washington. From my
26 investigation, it appears that the proprietor of Pinnacle Health PS Brad Ulrich. .

27 31. As outlined above, multiple sources of information indicate that someone
28 residing at the SUBJECT PREMISES used a computer connected to the internet via the

1 SUBJECT IP ADDRESS to share files depicting minors engage in sexually explicit
2 conduct on the BitTorrent P2P Network. Given the above facts and the information
3 contained in this Affidavit, I therefore believe there is probable cause to search the
4 SUBJECT PREMISES and any digital devices found therein for evidence, fruits, and
5 instrumentalities of the TARGET OFFENSES.

6 **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

7 32. As part of my training and experience, I have become familiar with the
8 Internet, a global network of computers and other electronic devices that communicate
9 with each other using various means, including standard telephone lines, high speed
10 telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions,
11 including satellite. Due to the structure of the Internet, connections between computers
12 on the Internet routinely cross state and international borders, even when the computers
13 communicating with each other are in the same state. Individuals and entities use the
14 Internet to gain access to a wide variety of information; to send information to, and
15 receive information from, other individuals; to conduct commercial transactions; and to
16 communicate via email.

17 33. Based on my training and experience, that cellular phones (referred to
18 herein generally as "smart phones") have the capability to access the Internet and store
19 information, such as videos and images. As a result, an individual using a smart phone
20 can send, receive, and store files, including child pornography, without accessing a
21 personal computer or laptop. An individual using a smart phone can also easily plug the
22 device into a computer, via a USB cable, and transfer data files from one digital device to
23 another. Many people generally carry their smart phone on their person; recent
24 investigations in this District have resulted in the discovery of child pornography files on
25 smart phones which were carried on an individual's person at the time the phones were
26 seized.

27 34. As set forth above and in Attachment B to this Affidavit, I seek permission
28 to search for and seize evidence, fruits, and instrumentalities of the above-referenced

1 crimes that might be at the SUBJECT PREMISES, in whatever form they are found. It
2 has been my experience that individuals involved in child pornography often prefer to
3 store child pornography in electronic form. The ability to store child pornography in
4 electronic form makes digital devices an ideal repository for child pornography because
5 the images can be easily sent or received over the Internet. As a result, one form in
6 which these items may be found is as electronic evidence stored on a digital device.

7 35. Based upon my knowledge, training, and experience in child exploitation
8 and child pornography investigations, and the experience and training of other law
9 enforcement officers with whom I have had discussions, I know that computers and
10 computer technology have revolutionized the way in which child pornography is
11 collected, distributed, and produced. Prior to the advent of computers and the Internet,
12 child pornography was produced using cameras and film, resulting in either still
13 photographs or movies. The photographs required darkroom facilities and a significant
14 amount of skill in order to develop and reproduce the images. As a result, there were
15 definable costs involved with the production of pornographic images. To distribute these
16 images on any scale also required significant resources. The photographs themselves
17 were somewhat bulky and required secure storage to prevent their exposure to the public.
18 The distribution of these images was accomplished through a combination of personal
19 contacts, mailings, and telephone calls, and compensation would follow the same paths.
20 More recently, through the use of computers and the Internet, distributors of child
21 pornography use membership based/subscription based websites to conduct business,
22 allowing them to remain relatively anonymous.

23 36. In addition, based upon my own knowledge, training, and experience in
24 child exploitation and child pornography investigations, and the experience and training
25 of other law enforcement officers with whom I have had discussions, I know that the
26 development of computers has also revolutionized the way in which those who seek out
27 child pornography are able to obtain this material. Computers serve four basic functions
28 in connection with child pornography: production, communication, distribution, and

1 storage. More specifically, the development of computers has changed the methods used
2 by those who seek to obtain access to child pornography as described in this Affidavit.

3 37. Producers of child pornography can now produce both still and moving
4 images directly from the average video or digital camera. These still and/or moving
5 images are then uploaded from the camera to the computer, either by attaching the
6 camera to the computer through a USB cable or similar device, or by ejecting the camera
7 memory card from the camera and inserting it into a card reader. Once uploaded to the
8 computer, the images can then be stored, manipulated, transferred, or printed directly
9 from the computer. Images can be edited in ways similar to those by which a photograph
10 may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated.
11 Producers of child pornography can also use a scanner to transfer printed photographs
12 into a computer-readable format. As a result of this technology, it is relatively
13 inexpensive and technically easy to produce, store, and distribute child pornography. In
14 addition, there is an added benefit to the pornographer in that this method of production
15 does not leave as large a trail for law enforcement to follow.

16 38. The Internet allows any computer to connect to another computer. By
17 connecting to a host computer, electronic contact can be made to literally millions of
18 computers around the world. A host computer is one that is attached to a network and
19 serves many users. Host computers, including ISPs, allow email service between
20 subscribers and sometimes between their own subscribers and those of other networks.
21 In addition, these service providers act as a gateway for their subscribers to the Internet.
22 Having said that, however, this application does not seek to reach any host computers.

23 39. The Internet allows users, while still maintaining anonymity, to easily
24 locate (i) other individuals with similar interests in child pornography, and (ii) websites
25 that offer child pornography. Those who seek to obtain images or videos of child
26 pornography can use standard Internet connections, such as those provided by businesses,
27 universities, and government agencies, to communicate with each other and to distribute
28 child pornography. These communication links allow contacts around the world as easily

1 as calling next door. Additionally, these communications can be quick, relatively secure,
2 and as anonymous as desired. All of these advantages, which promote anonymity for
3 both the distributor and recipient, are well known and are the foundation of transactions
4 involving those who wish to gain access to child pornography over the Internet.
5 Sometimes the only way to identify both parties and verify the transportation of child
6 pornography over the Internet is to examine the distributors/recipient's computer,
7 including the Internet history and cache to look for "footprints" of the websites and
8 images accessed by the distributor/recipient.

9 40. The computer's capability to store visual depictions in digital form makes it
10 an ideal repository for child pornography. The size of the electronic storage media
11 (commonly referred to as a "hard drive") used in home computers has grown
12 tremendously within the last several years. Hard drives with the capacity of 2 terabytes
13 are not uncommon. These drives can store thousands of images at very high resolution.
14 Magnetic storage located in host computers adds another dimension to the equation. It is
15 possible to use a video camera to capture an image, process that image in a computer
16 with a video capture board, and save that image to storage elsewhere. Once this is done,
17 there is no readily apparent evidence at the "scene of the crime." Only with careful
18 laboratory examination of electronic storage devices is it possible to recreate the evidence
19 trail.

20 41. Based upon my knowledge, experience, and training in child pornography
21 investigations, and the training and experience of other law enforcement officers with
22 whom I have had discussions, I know that there are certain characteristics common to
23 individuals who have a sexualized interest in children and depictions of children:

24 a. They may receive sexual gratification, stimulation, and satisfaction
25 from contact with children; or from fantasies they may have viewing children engaged in
26 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other
visual media; or from literature describing such activity.

27 b. They may collect sexually explicit or suggestive materials in a
28 variety of media, including photographs, magazines, motion pictures, videotapes, books,

1 slides, and/or drawings or other visual media. Such individuals often times use these
2 materials for their own sexual arousal and gratification. Further, they may use these
3 materials to lower the inhibitions of children they are attempting to seduce, to arouse the
4 selected child partner, or to demonstrate the desired sexual acts. These individuals may
5 keep records, to include names, contact information, and/or dates of these interactions, of
6 the children they have attempted to seduce, arouse, or with whom they have engaged in
7 the desired sexual acts.

8 c. They often maintain any "hard copies" of child pornographic
9 material that is, their pictures, films, video tapes, magazines, negatives, photographs,
10 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of
11 their home or some other secure location. These individuals typically retain these "hard
12 copies" of child pornographic material for many years, as they are highly valued.

13 d. Likewise, they often maintain their child pornography collections
14 that are in a digital or electronic format in a safe, secure and private environment, such as
15 a computer and surrounding area. These collections are often maintained for several
16 years and are kept close by, often at the individual's residence or some otherwise easily
17 accessible location, to enable the owner to view the collection, which is valued highly.
18 They also may opt to store the contraband in cloud accounts. Cloud storage is a model of
19 data storage where the digital data is stored in logical pools, the physical storage can span
20 multiple servers, and often locations, and the physical environment is typically owned
21 and managed by a hosting company. Cloud storage allows the offender ready access to
22 the material from any device that has an Internet connection, worldwide, while also
23 attempting to obfuscate or limit the criminality of possession as the material is stored
24 remotely and not on the offender's device.]

25 e. They also may correspond with and/or meet others to share
26 information and materials; rarely destroy correspondence from other child pornography
27 distributors/collectors; conceal such correspondence as they do their sexually explicit
28 material; and often maintain lists of names, addresses, and telephone numbers of
individuals with whom they have been in contact and who share the same interests in
child pornography.

f. They generally prefer not to be without their child pornography for
any prolonged time period. This behavior has been documented by law enforcement
officers involved in the investigation of child pornography throughout the world.

42. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

43. Given the above-stated facts and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe the person who used a computer to share files of child pornography from the SUBJECT IP ADDRESS likely has a sexualized interest in children and depictions of children and that evidence of child pornography is likely to be found at the SUBJECT PREMISES.

FRUITS, EVIDENCE, AND INSTRUMENTALITIES INSIDE THE SUBJECT PREMISES AND ANY CLOSED CONTAINERS AND ELECTRONIC DEVICES FOUND THEREIN

1. As described above and in Attachment B, this application seeks permission to search for and seize items listed in Attachment B that might be found in the SUBJECT PREMISES, in whatever form they are found. One form in which evidence, fruits, or instrumentalities might be found is data stored on a computer's hard drive or other digital

1 device¹ or electronic storage media.² Thus, the warrant applied for would authorize the
 2 seizure of electronic storage media or, potentially, the copying of electronically stored
 3 information, all under Rule 41(e)(2)(B).

4 2. Through my training and experience, and the information learned during
 5 the course of this investigation, I know that individuals who engage in child pornography
 6 offenses often keep physical evidence, fruits, and instrumentalities of their crimes inside
 7 their residences, including but not limited to, digital devices

8 3. *Probable cause.* Based upon my review of the evidence gathered in this
 9 investigation, my review of data and records, information received from other agents and
 10 computer forensic examiners, and my training and experience, I submit that if a digital
 11 device or other electronic storage medium is found in the SUBJECT PREMISES, there is
 12 probable cause to believe that evidence, fruits, and instrumentalities of the TARGET
 13 OFFENSES will be stored on those digital devices or other electronic storage media,
 14 because a computer or digital device at SUBJECT PREMISES was utilized to connect to
 15 the Internet and distribute child pornography via a P2P network. There is, therefore,
 16 probable cause to believe that evidence, fruits, and instrumentalities, of the crimes under
 17 investigation exist and will be found on digital devices or other electronic storage media
 18 at the SUBJECT PREMISES, for at least the following reasons:

19 a. Based my knowledge, training, and experience, I know that
 20 computer files or remnants of such files may be recovered months or even years after
 21 they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

22 ¹ “Digital device” includes any device capable of processing and/or storing data in electronic
 23 form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet
 24 computers, computer servers, peripheral input/output devices such as keyboards, printers,
 25 scanners, plotters, monitors, and drives intended for removable media, related communications
 26 devices such as modems, routers and switches, and electronic/digital security devices, wireless
 27 communication devices such as mobile or cellular telephones and telephone paging devices,
 28 personal data assistants (“PDAs”), iPods/iPads, Blackberries, digital cameras, digital gaming
 devices, global positioning satellite devices (GPS), or portable media players.

² Electronic Storage media is any physical object upon which electronically stored information
 can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs,
 and other magnetic or optical media.

1 Electronic files downloaded to a storage medium can be stored for years at little or no
2 cost. Even when files have been deleted, this information can sometimes be recovered
3 months or years later with forensics tools. This is because when a person “deletes” a file
4 on a computer, the data contained in the files does not actually disappear; rather, that data
5 remains on the storage medium until it is overwritten by new data.

6 b. Therefore, deleted files, or remnants of deleted files, may reside in
7 free space or slack space—that is, in space on the storage medium that is not currently
8 being used by an active file—for long periods of time before they are overwritten. In
9 addition, a computer’s operating system may also keep a record of deleted data in “swap”
10 or “recovery” files.

11 c. Wholly apart from user-generated files, computer storage media—in
12 particular, computers’ internal hard drives—contain electronic evidence of how a
13 computer has been used, what it has been used for, and who has used it. To give a few
14 examples, this forensic evidence can take the form of operating system configurations,
15 artifacts from operating system or application operation, file system data structures, and
16 virtual memory “swap” paging files. Computer users typically do not erase or delete this
17 evidence, because special software is typically required for that task. However, it is
18 technically possible to delete this information.

19 d. Similarly, files that have been viewed via the Internet are sometimes
20 automatically downloaded into a temporary Internet directory or “cache.”

21 e. Digital storage devices may also be large in capacity, but small in
22 physical size. Because those who are in possession of such devices also tend to keep
23 them on their persons, especially when they may contain evidence of a crime. Digital
24 storage devices may be smaller than a postal stamp in size, and thus they may easily be
25 hidden in a person’s pocket.

26 4. As further described in Attachment B, this application seeks permission to
27 locate not only computer files that might serve as direct evidence of the crimes described
28 on the warrant, but also for forensic electronic evidence that establishes how computers
were used, the purpose of their use, who used them, and when. There is probable cause
to believe that this forensic electronic evidence will be on digital devices found in the
SUBJECT PREMISES because:

a. Data on the digital storage medium or digital devices can provide
evidence of a file that was once on the digital storage medium or digital devices but has

1 since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has
2 been deleted from a word processing file). Virtual memory paging systems can leave
3 traces of information on the storage medium that show what tasks and processes were
4 recently active. Web browsers, e-mail programs, and chat programs store configuration
5 information on the storage medium that can reveal information such as online nicknames
6 and passwords. Operating systems can record additional information, such as the
7 attachment of peripherals, the attachment of USB flash storage devices or other external
8 storage media, and the times the computer was in use. Computer file systems can record
9 information about the dates files were created and the sequence in which they were
10 created, although this information can later be falsified.

11 b. As explained herein, information stored within a computer and other
12 electronic storage media may provide crucial evidence of the “who, what, why, when,
13 where, and how” of the criminal conduct under investigation, thus enabling the United
14 States to further establish and prove each element or alternatively, to exclude the innocent
15 from further suspicion. In my training and experience, information stored within a
16 computer or storage media (e.g. registry information, communications, images and
17 movies, transactional information, records of session times and durations, Internet
18 history, and anti-virus, spyware, and malware detection programs) can indicate who has
19 used or controlled the computer or storage media. This “user attribution” evidence is
20 analogous to the search of “indicia of occupancy” while executing a search warrant at a
21 residence. The existence or absence of anti-virus, spyware, and malware detection
22 programs may indicate whether the computer was remotely accessed, thus inculcating or
23 exculpating the computer owner. Further computer and storage media activity can
24 indicate how and when the computer or storage media was accessed or used. For
25 example, as described herein, computers typically contain information that log: computer
26 activity associated with user accounts and electronic storage media that connected with
27 the computer. Such information allows investigators to understand the chronological
28 context of computer or electronic storage media access, use, and events relating to the
crime under investigation. Additionally, some information stored within a computer or
electronic storage media may provide crucial evidence relating to the physical location of
other evidence and the suspect. For example, images stored on a computer may both
show a particular location and have geolocation information incorporated into its file
data. Such file data typically also contains information indicating when the file or image
was created. The existence of such image files, along with external device connection
logs, may also indicate the presence of additional electronic storage media (e.g., a digital
camera or cellular phone with an incorporated camera). The geographic and timeline
information described herein may either inculcate or exculpate the computer user. Last,
information stored within a computer may provide relevant insight into the computer
user’s state of mind as it relates to the offense under investigation. For example,
information within the computer may indicate the owner’s motive and intent to commit

1 the crime (e.g. Internet searches indicating criminal planning), or consciousness of guilt
 2 (e.g., running a “wiping” program to destroy evidence on the computer or password
 3 protecting/encrypting such evidence in an effort to conceal it from law enforcement).

4 c. A person with appropriate familiarity with how a computer works
 5 can, after examining this forensic evidence in its proper content, draw conclusions about
 6 how computers were used, the purpose of their use, who used them, and when.

7 d. The process of identifying the exact files, blocks, registry entries,
 8 logs, or other forms of forensic evidence on a storage medium that are necessary to draw
 9 an accurate conclusion is a dynamic process. While it is possible to specify in advance
 10 the records to be sought, computer evidence is not always data that can be merely
 11 reviewed by a review team and passed along to investigators. Whether data stored on a
 12 computer is evidence may depend on other information stored on the computer and the
 13 application of knowledge about how a computer behaves. Therefore, contextual
 14 information necessary to understand other evidence also falls within the scope of the
 15 warrant.

16 e. Further, in finding evidence of how a computer was used, the
 17 purpose of its use, who used it, and when, sometimes it is necessary to establish that a
 18 particular thing is not present on a storage medium. For example, the presence or
 19 absence of counter-forensic programs or anti-virus programs (and associated data) may
 20 be relevant to establishing a user’s intent.

21 f. I know that when an individual uses a computer to store, receive, or
 22 distribute child pornography, the individual’s computer or digital device will generally
 23 serve both as an instrumentality for committing the crime, and also as a storage medium
 24 for evidence of the crime. The computer or digital device is an instrumentality of the
 25 crime because it is used as a means of committing the criminal offense. The computer or
 26 digital device is also likely to be a storage medium for evidence of crime. From my
 27 training and experience, I believe that a computer or digital device used to commit a
 28 crime of this type may contain: data that is evidence of how the computer was used; data
 that was sent or received; notes as to how the criminal conduct was achieved; records of
 text discussions about the crime; and other records that indicate the nature of the offense.

5. *Necessity of seizing or copying entire computers or storage medium.* In
 most cases, a thorough search of a premises for information that might be stored on
 digital storage media or other digital devices often requires the seizure of the digital
 devices and digital storage media for later off-site review consistent with the warrant. In
 lieu of removing storage media from the premises, it is sometimes possible to make an

1 image copy of storage media. Generally speaking, imaging is the taking of a complete
2 electronic copy of the digital media's data, including all hidden sectors and deleted files.
3 Either seizure or imaging is often necessary to ensure the accuracy and completeness of
4 data recorded on the storage media, and to prevent the loss of the data either from
5 accidental or intentional destruction. This is true because of the following:

6 a. *The time required for an examination.* As noted above, not all
7 evidence takes the form of documents and files that can be easily viewed on site.
8 Analyzing evidence of how a computer has been used, what it has been used for, and who
9 has used it requires considerable time, and taking that much time on premises could be
10 unreasonable. As explained above, because the warrant calls for forensic electronic
11 evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage
12 media to obtain evidence. Storage media can store a large volume of information.
13 Reviewing that information for things described in the warrant can take weeks or months,
14 depending on the volume of data stored, and would be impractical and invasive to
15 attempt on-site.

16 b. *Technical requirements.* Computers can be configured in several
17 different ways, featuring a variety of different operating systems, application software,
18 and configurations. Therefore, searching them sometimes requires tools or knowledge
19 that might not be present on the search site. The vast array of computer hardware and
20 software available makes it difficult to know before a search what tools or knowledge
21 will be required to analyze the system and its data on-site. However, taking the storage
22 media off-site and reviewing it in a controlled environment will allow its examination
23 with the proper tools and knowledge.

24 c. *Variety of forms of electronic media.* Records sought under this
25 warrant could be stored in a variety of storage media formats that may require off-site
26 reviewing with specialized forensic tools.

27 6. Searching computer systems is a highly technical process that requires
28 specific expertise and specialized equipment. There are so many types of computer
hardware and software in use today that it is rarely possible to bring to the search site all
the necessary technical manuals and specialized equipment necessary to consult with
computer personnel who have expertise in the type of computer, operating system, or
software application being searched.

1 7. The analysis of computer systems and storage media often relies on
2 rigorous procedures designed to maintain the integrity of the evidence and to recover
3 “hidden,” mislabeled, deceptively named, erased, compressed, encrypted or password-
4 protected data, while reducing the likelihood of inadvertent or intentional loss or
5 modification of data. A controlled environment such as a laboratory, is typically required
6 to conduct such an analysis properly.

7 8. The volume of data stored on many computer systems and storage devices
8 will typically be so large that it will be highly impracticable to search for data during the
9 execution of the physical search of the premises. The hard drives commonly included in
10 desktop and laptop computers are capable of storing millions of pages of text.

11 9. A search of digital devices for evidence described in Attachment B may
12 require a range of data analysis techniques. In some cases, agents may recover evidence
13 with carefully targeted searches to locate evidence without requirement of a manual
14 search through unrelated materials that may be commingled with criminal evidence.
15 Agents may be able to execute a “keyword” search that searches through the files stored
16 in a digital device for special terms that appear only in the materials covered by the
17 warrant. Or, agents may be able to locate the materials covered by looking for a
18 particular directory or name. However, in other cases, such techniques may not yield the
19 evidence described in the warrant. Individuals may mislabel or hide files and directories;
20 encode communications to avoid using keywords; attempt to delete files to evade
21 detection; or take other steps designed to hide information from law enforcement
22 searches for information.

23 10. The search procedure of any digital device seized may include the
24 following on-site techniques to seize the evidence authorized in Attachment B:

25 a. On-site triage of computer systems to determine what, if any,
26 peripheral devices or digital storage units have been connected to such computer systems,
27 a preliminary scan of image files contained on such systems and digital storage devices to
28 help identify any other relevant evidence or co-conspirators.

1 b. On-site copying and analysis of volatile memory, which is usually
2 lost if a computer is powered down, and may contain information about how the
3 computer is being used, by whom, when and may contain information about encryption,
4 virtual machines, or stenography which will be lost if the computer is powered down.

5 c. On-site forensic imaging of any computers may be necessary for
6 computers or devices that may be partially or fully encrypted in order to preserve
7 unencrypted data that may, if not immediately imaged on-scene become encrypted and
8 accordingly become unavailable for any examination.

9 11. *Nature of examination.* Based on the foregoing, and consistent with Rule
10 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise
11 copying storage media that reasonably appear to contain some or all of the evidence
12 described in the warrant, and would authorize a later review of the media or information
13 consistent with the warrant. The later review may require techniques, including but not
14 limited to computer-assisted scans of the entire medium, that might expose many parts of
15 a hard drive to human inspection in order to determine whether it is evidence described
16 by the warrant.
17
18
19
20
21
22
23
24
25
26
27
28

CONCLUSION

12. Based on the information set forth herein, there is probable cause to search the above described SUBJECT PREMISES, as further described in Attachment A, as well as on and in any digital device or other electronic storage media found at the SUBJECT PREMISES for evidence, fruits and instrumentalities, as further described in Attachment B, of the TARGET OFFENSES .



Ingrid Arbuthnot-Stohl, Affiant
Special Agent, FBI

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit this 29th day of June, 2020.



MICHELLE L. PETERSON
United States Magistrate Judge

ATTACHMENT A
(SUBJECT PREMISES)

The physical address of the SUBJECT PREMISES is 13742 97th Ave., NE, Kirkland, WA 98034, and is more fully described as a property containing a two-story, single-family home with an attached carport, yellow-orangish and blue color siding with white trim. The front door is located off of the carport with a small box to the side of the door and the numbers 13742 on a plaque above the box. The residence is at the end of a cul-de-sac.



1 The search is to include all rooms, persons, garages, vehicles, or outbuildings
2 located on the SUBJECT PREMISES, as well as any digital device(s) or other electronic
3 storage media found therein or thereon.
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT B**(PROPERTY TO BE SEIZED)**

Evidence, fruits, and instrumentalities of violations 18 U.S.C. §§ 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), as follows:

- a. Items, records, or information³ relating to visual depictions of minors engaged in sexually explicit conduct;
- b. Items, records, or information relating to the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;
- c. Items, records, or information concerning communications about the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;
- d. Items, records, or information concerning communications about the sexual abuse or exploitation of minors;
- e. Items, records, or information related to communications with or about minors;
- f. Items, records, or information concerning the identities and contact information (including mailing addresses) of any individuals involved in the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct, saved in any form;
- g. Items, records, or information concerning occupancy, residency or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence,

³ As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

1 purchase or lease agreements, diaries, statements, identification documents,
2 address books, telephone directories, and keys;

3 h. Items, records, or information concerning the ownership or use of computer
4 equipment found in the SUBJECT PREMISES, including, but not limited
5 to, sales receipts, bills for internet access, handwritten notes, and computer
6 manuals;

7 i. Any digital devices or other electronic storage media⁴ and/or their
8 components including:

9 i. any digital device or other electronic storage media capable of being
10 used to commit, further, or store evidence, fruits, or instrumentalities
11 of the offenses listed above;

12 ii. any magnetic, electronic or optical storage device capable of storing
13 data, including thumb drives, SD cards, or external hard drives;

14 iii. any physical keys, encryption devices, dongles and similar physical
15 items that are necessary to gain access to the computer equipment,
16 storage devices or data; and

17 iv. any passwords, password files, test keys, encryption codes or other
18 information necessary to access the computer equipment, storage
19 devices or data.

20 j. For any digital device or other electronic storage media whose seizure is
21 otherwise authorized by this warrant, and any digital device or other
22 electronic storage media that contains or in which is stored records or
23 information that is otherwise called for by this warrant:

24 i. evidence of who used, owned, or controlled the digital device or
25 other electronic storage media at the time the things described in this
26 warrant were created, edited, or deleted, such as logs, registry
27

28 ⁴ The term “digital devices” includes all types of electronic, magnetic, optical, electrochemical,
or other high speed data processing devices performing logical, arithmetic, or storage functions,
including desktop computers, notebook computers, mobile phones, tablets, server computers, and
network hardware. The term “electronic storage media” includes any physical object upon
which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash
memory, CD-ROMs, and other magnetic or optical media.

1 entries, configuration files, saved usernames and passwords,
2 documents, browsing history, user profiles, email, email contacts,
3 “chat,” instant messaging logs, photographs, and correspondence;

4 ii. evidence of software that would allow others to control the digital
5 device or other electronic storage media, such as viruses, Trojan
6 horses, and other forms of malicious software, as well as evidence of
7 the presence or absence of security software designed to detect
8 malicious software;

9 iii. evidence of the lack of such malicious software;

10 iv. evidence of the attachment to the digital device of other storage
11 devices or similar containers for electronic evidence;

12 v. evidence of counter-forensic programs (and associated data) that are
13 designed to eliminate data from the digital device or other electronic
14 storage media;

15 vi. evidence of the times the digital device or other electronic storage
16 media was used;

17 vii. passwords, encryption keys, and other access devices that may be
18 necessary to access the digital device or other electronic storage
19 media;

20 viii. documentation and manuals that may be necessary to access the
21 digital device or other electronic storage media or to conduct a
22 forensic examination of the digital device or other electronic storage
23 media;

24 ix. records of or information about the Internet Protocol used by the
25 digital device or other electronic storage media;

26 x. records of internet activity, including firewall logs, caches, browser
27 history and cookies, “bookmarked” or “favorite” web pages, search
28 terms that the user entered into any internet search engine, and
records of user-typed web addresses.

xi. contextual information necessary to understand the evidence
described in this attachment.

1 This warrant authorizes a review of electronic storage media and electronically
2 stored information seized or copied pursuant to this warrant in order to locate evidence,
3 fruits, and instrumentalities described in this warrant. The review of this electronic data
4 may be conducted by any government personnel assisting in the investigation, who may
5 include, in addition to law enforcement officers and agents, attorneys for the government,
6 attorney support staff, and technical experts. Pursuant to this warrant, the FBI may
7 deliver a complete copy of the seized or copied electronic data to the custody and control
8 of attorneys for the government and their support staff for their independent review.

9 THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE
10 MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS
11 SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO
12 THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC
13 STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL
14 ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE
15 CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR
16 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED
17 CRIMES.
18
19
20
21
22
23
24
25
26
27
28